



HAL
open science

Les conséquences humaines de l'échange transnational des données individuelles

Didier Bigo, Pierre Piazza

► **To cite this version:**

Didier Bigo, Pierre Piazza. Les conséquences humaines de l'échange transnational des données individuelles. *Cultures & conflits*, 2009, 4 (76), pp.7-14. 10.4000/conflits.17755 . hal-01022639

HAL Id: hal-01022639

<https://sciencespo.hal.science/hal-01022639>

Submitted on 10 Jul 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Didier BIGO et Pierre Piazza

Editorial

Les conséquences humaines de l'échange transnational des données individuelles

Avertissement

Le contenu de ce site relève de la législation française sur la propriété intellectuelle et est la propriété exclusive de l'éditeur.

Les œuvres figurant sur ce site peuvent être consultées et reproduites sur un support papier ou numérique sous réserve qu'elles soient strictement réservées à un usage soit personnel, soit scientifique ou pédagogique excluant toute exploitation commerciale. La reproduction devra obligatoirement mentionner l'éditeur, le nom de la revue, l'auteur et la référence du document.

Toute autre reproduction est interdite sauf accord préalable de l'éditeur, en dehors des cas prévus par la législation en vigueur en France.

revues.org

Revues.org est un portail de revues en sciences humaines et sociales développé par le Cléo, Centre pour l'édition électronique ouverte (CNRS, EHESS, UP, UAPV).

Référence électronique

Didier BIGO et Pierre Piazza, « Les conséquences humaines de l'échange transnational des données individuelles », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011, consulté le 03 janvier 2013. URL : <http://conflits.revues.org/17755>

Éditeur : Centre d'études sur les conflits

<http://conflits.revues.org>

<http://www.revues.org>

Document accessible en ligne sur : <http://conflits.revues.org/17755>

Ce document est le fac-similé de l'édition papier.

Creative Commons License

Les conséquences humaines de l'échange transnational des données individuelles

Didier BIGO et Pierre PIAZZA

A l'échelon transnational, le partage d'informations sur des personnes s'accélère et s'amplifie ¹. Présenté comme un indispensable impératif pour faire face efficacement à des risques et des menaces susceptibles de saper les fondements de la démocratie (terrorisme, criminalité organisée, immigration illégale, fraudes, etc.), cet échange emprunte une multitude de canaux communicationnels et institutionnels, et utilise des dispositifs technologiques de traçabilité et d'anticipation. L'interconnexion observable entre bases de données contenant des informations personnelles ou des profils anonymisés, et servant à élaborer des listes d'individus à surveiller, s'opère normalement à travers des circuits officiels de justice criminelle, de contrôle des frontières et de surveillance des flux de capitaux. Mais au nom de la lutte antiterroriste et du renseignement préventif, les règles de contrôle – judiciaires ou parlementaires – qui les régissent ont été assouplies et on a vu se multiplier les canaux officieux entre acteurs du renseignement ². Ce phénomène se constate à l'échelle locale et régionale avec les croisements de fichiers, ou tout simplement *via* les rencontres entre personnels venant des services de police, des services sociaux ou des mairies ; à l'échelle nationale avec l'intégrations de fichiers relevant de services de police et d'immigration différents ³ ; à l'échelle européenne avec les

-
1. Bigo D., Walker R.B.J., « Le régime du contre-terrorisme global », in Bigo D., Bonelli L., Deltombe T. (dir.), *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, Paris, La Découverte, 2008, pp. 13-35.
 2. Le directeur de la National Security Agency (NSA) américaine ne s'en est pas caché et a évoqué des « clubs de rencontre » entre services de renseignements. Le Club de Berne a été réactif et il a été question de l'officialiser sous le terme EuroRens. Cependant, et malgré les efforts du coordinateur antiterroriste européen, le projet a avorté, plusieurs services refusant toute officialisation et toute « publicité ». Entretiens de Didier Bigo avec des responsables antiterroristes menés en juin 2009.
 3. Voir les travaux parlementaires relatifs aux crédits alloués par la loi de finance 2009 aux missions « Sécurité » et « Immigration, asile et intégration », <http://www.senat.fr/rap/a08-104-11/a08-104-115.html>. Pour une liste des fichiers en France, voir le rapport au ministre de l'Intérieur, Bauer A., Soullez C., Ventre A-M., *Mieux contrôler les fichiers de police pour protéger les libertés*, Paris, La documentation française, 2009 ; et pour une approche plus soucieuse des libertés, voir Preuss-Laussinotte S., *L'essentiel des libertés et droits fondamentaux, tome 1, L'organisation des Libertés*, Paris, Gualino éditeur, 2001.

bases de données Eurodac ou Europol ; à l'échelle transatlantique avec des échanges formels et informels accélérant la circulation des informations ; à l'échelle internationale, enfin, avec la participation de régimes non démocratiques ⁴. La croyance en une possible prévention des comportements humains agressifs *via* une information à la fois totale, ciblée et en temps réel, a amené à faire confiance à des technologies qui prétendent pouvoir combattre l'incertitude en anticipant le pire des futurs et en le corrigeant avant qu'il n'advienne. La liste des technologies et surtout leur mise en réseau est maintenant considérable et nous n'en connaissons au quotidien que quelques rares éléments : *Passengers Name Records* dans les aéroports, visas d'entrée et de sortie électronique, passeports avec identifiants biométriques dynamiques, blocage de cartes de crédit à l'étranger, etc. Pourtant, la panoplie s'étend de la surveillance des conversations jusqu'aux drones visant à tuer à distance, en passant par des reconfigurations des états psychologiques de consommation et de citoyenneté ⁵. Sans même parler des pratiques illégales qui ont accompagné cette recherche d'information tout azimut – attribuées le plus souvent à des agents trop zélés – la logique même qui sous-tend le système est problématique au regard des libertés publiques. En effet, ces échanges de données à l'échelle transnationale ont eu tendance à décontextualiser les informations, à les agréger de manière parfois erronée, et à créer des erreurs de jugement entraînant des conséquences humaines graves pour les individus qui en sont victimes.

Ce ne sont pas des gênes passagères auxquelles on pourrait s'accoutumer en contrepartie d'une sécurité plus grande : il en va de la vie de personnes, de leurs détentions indéfinies et de pratiques arbitraires répétées limitant la confiance des citoyens dans leurs institutions. Il ne s'agit pas non plus de quelques incidents isolés ou même d'une entrée somnambulique dans une société de surveillance, mais plutôt d'une reconfiguration de celle-ci en une société internationale de suspicion visant à tenir à l'écart, à renvoyer ou à punir sans procès, des populations considérées « dangereuses » par des réseaux d'experts qui s'accordent sur les arbitrages et les contours de cette « dangerosité ». Ceci implique désormais un nombre croissant de contacts entre bureaucraties étatiques (services de renseignement, de police criminelle, d'immigration, de contrôle des frontières, magistrats, etc.) et l'établissement de lieux privilégiés supranationaux (G8-groupe de Lyon, Interpol, réseau EU-FBI, OTAN, Europol, Eurojust, Frontex, Siten, etc.), de même que la multiplication des interactions avec des acteurs privés, sans que les responsabilités de chacun puissent être clairement identifiées. Il est rare en pratique que l'on puisse reconstituer *a posteriori* qui, parmi les autorités compétentes, a agrégé,

4. Voir les travaux menés dans le cadre du programme *The Changing Landscape of European Security* (Challenge) PCRD6 de la Commission européenne, dont les premiers résultats ont été publiés dans Bigo D. *et al.*, *The Field of the EU Internal Security Agencies*, Paris, L'Harmattan, 2008.

5. Chardel P-A., Rockhill G. (dir.), *Technologies de contrôle dans la mondialisation. Enjeux politiques, éthiques et esthétiques*, Paris, Kimé, 2010.

classé, trié, exclu, hiérarchisé, construit le renseignement à partir de données diverses, comme la validité de ces dernières.

La hiérarchie momentanée des dangers et risques à prévenir et des groupes à protéger peut ainsi provenir de cette guilda transnationale des professionnels de l'(in)sécurité et/ou des arbitrages des professionnels de la politique, agissant plutôt à l'échelle nationale. Les enquêtes récentes sur les modalités d'entrée en guerre ou de surveillance interne des populations de la période 2001-2005 montrent clairement cette interface ⁶.

Les informations collectées peuvent concerner une population isolée à partir de critères spécifiques (nationalité, religion, ethnicité, politique, choix alimentaires, cartes de crédit d'une banque spécifique, etc.) ou revêtir un caractère personnel lorsqu'il s'agit d'un individu particulier déjà connu des autorités. Dans les deux cas, une logique proactive d'anticipation des comportements (*data mining*, profilage, etc.) débouche sur la constitution de « listes de suspects potentiels » sur lesquels faire porter un contrôle approfondi. Tout se passe comme si l'inscription informatisée de données ne débouchait pas sur la nécessité d'un complément d'enquête mais sur une forme de pré-culpabilité.

Ce numéro de *Cultures & Conflits* entend approfondir les formes de la gouvernementalité contemporaine par l'inquiétude. Il entre en résonance avec plusieurs numéros précédents ⁷, mais porte très spécifiquement sur les conséquences néfastes que peut produire pour les individus cette intensification de l'échange et de l'exploitation d'informations relatives à leur être, leurs actes et leurs avoirs.

L'actualité ne cesse de rappeler la nécessité d'une analyse en profondeur de cette modalité du contre-terrorisme global. L'arrestation d'Umar Farouk Abdulmutallab, l'auteur présumé de l'attentat manqué du 25 décembre 2009 contre un vol Amsterdam-Détroit de la Northwest Airlines, pose ainsi bien des questions sur la validité de ces échanges massifs d'informations et sur leur pertinence, tout comme la détention d'un enfant de 8 ans pendant 24 heures car son nom ressemblait à celle d'un terroriste connu, ou bien le rejet de l'accord SWIFT par le Parlement européen au début du mois de février 2010 afin

-
6. Voir, au Royaume-Uni, la commission d'enquête de Sir John Chilcot sur l'engagement britannique en Irak, et aux Pays-Bas, la commission d'enquête indépendante de Willibrord Davids qui a considéré que la légitimation de l'invasion « n'était pas suffisante ». Sur le réseau échelon, voir Campbell D. et Esquié H., *Surveillance électronique planétaire*, Paris, Editions Allia, 2006.
7. Voir notamment les numéros 74, « Sécurité et protection des données » (été 2009) ; 68, « Circulation et archipels de l'exception » (hiver 2007) ; 64, « Identifier et surveiller » (hiver 2006) ; 63, « Mort volontaire combattante (automne 2006) » ; 62, « Arrêter et juger en Europe » (printemps 2006) ; 61, « Antiterrorisme et société » (printemps 2006) et 58, « Suspicion et exception » (été 2005). Ils sont désormais accessibles sur <http://www.cairn.info/revue-cultures-et-conflits.htm>

d'éviter que les services de renseignements américains (et européens) aient accès aussi facilement aux informations bancaires des citoyens européens ⁸.

Allons nous vers une limitation des pratiques les plus choquantes en terme de droits de l'Homme ou vers leur normalisation ? L'analyse des cas de Maher Arar, Abu Omar, Ahmed Agiza et Muhammad Alzery que nous avons récemment menée montre que les pratiques arbitraires découlant d'échanges d'informations à caractère personnel mal transmises ou interprétées systématiquement en défaveur de l'individu sont imbriquées dans une logique plus profonde de mobilité sous surveillance ⁹. Dick Marty rappelle ici même les cas d'Al Masri, Murat Journaz, Youssef Nada et insiste sur le fait que l'indifférence des médias et des hommes politiques à ces violations des droits tient sans doute malheureusement au fait qu'ils sont musulmans. Ce numéro a donc pour objectif de compléter l'analyse déjà entamée et d'initier une réflexion d'ensemble sur les conséquences néfastes d'un contre-terrorisme qui se veut global et qui tend à coloniser les activités les plus diverses de la vie sociale au nom de la prévention et de la sécurité maximale. Il s'agit sur le fond de remettre en cause l'idée que la sécurité n'aurait pas un coût extrêmement élevé pour nos sociétés et qu'elle serait par définition souhaitable et donc sans limite. Il s'agit également de questionner la croyance que les technologies contemporaines seraient à même de réguler la violence et les insécurités, par une suprématie informationnelle permettant d'anticiper et de prédire les menaces humaines ou même les hasards, dépolitisant par là même les rapports sociaux. Ces deux idées qui sont en train de s'imposer comme condition de possibilité des discours sur les libertés et la démocratie, sont éminemment problématiques, quand bien même elles sont reprises à l'unisson par les clubs d'experts internationaux sur la globalisation des menaces.

Ce ne sont pas pour autant des idées neuves, liées à des situations d'exception. Ce sont des idées qui refont surface et qui sont portées par des histoires et des trajectoires d'acteurs spécifiques. C'est pourquoi nous avons inclus dans ce numéro des articles de nature socio-historique permettant de mieux comprendre cet enjeu du présent à travers un regard porté sur des expériences passées. Les logiques de certaines de ces pratiques s'ancrent en effet dans une histoire longue dont les ressorts sont désormais mieux connus, notamment grâce aux travaux réalisés par quelques historiens. Ainsi, Vincent Denis a analysé de manière très détaillée comment dès le XVIII^e siècle en France, les pouvoirs publics ont commencé à mettre sur pied et à améliorer une multitude de systèmes d'enregistrement des individus en prenant alors pour cible privilégiées certaines catégories spécifiques de la population (mendiants, vagabonds, ouvriers, soldats, etc.) ¹⁰. Ici même, l'historien Ilse About rappelle pour sa

8. Pour d'autres exemples voir Bigo D., « Dans les filets du contre-terrorisme global », *Le Monde diplomatique*, octobre 2008.

9. Bigo D., Guittet E-P., Scherrer A., (dir.), *Mobilités sous surveillance*, Montréal, Athéna, 2010.

10. Denis V., *Une histoire de l'identité. France, 1715-1815*, Seyssel, Champ Vallon, 2008.

part de quelle manière se dessine progressivement en France, entre 1860 et 1930, un durcissement significatif des mesures adoptées à l'encontre des Tsiganes. Il montre à quel point devient alors primordial pour les forces de l'ordre l'enjeu de captation et d'échange de leurs données personnelles tant au niveau local et national que transnational. L'auteur expose les effets qu'induit au quotidien sur l'existence et la trajectoire des membres de cette population – officiellement désignée sous l'appellation « nomade » – l'exacerbation de la pression policière. Les obligeant à se soumettre à une batterie de nouvelles contraintes, le renforcement des dispositifs policiers d'identification, de contrôle et de traçabilité sert la mise en place d'un véritable quadrillage territorial aux maillages de plus en plus serrés qui transforme en profondeur leur mobilité, leur statut et la façon dont ils sont perçus. L'illusion de la nouveauté qui parfois conduit les « *surveillance studies* » à exagérer le poids des technologies récentes et à négliger les processus sociaux doit donc être dissipée. Ce qui est à l'œuvre est politique, pas seulement technologique. A cet égard, l'opportunité dont disposent aujourd'hui les chercheurs travaillant sur la thématique de l'identification de croiser leurs savoirs et leurs approches dans des réseaux académiques internationaux favorisant l'interdisciplinarité ¹¹, permet d'apporter d'autres précieux éclairages sur le caractère crucial des enjeux historiquement liés à ce phénomène au travers duquel se donnent à voir des manifestations tangibles du processus de consolidation du pouvoir d'Etat et des guildes transnationales des professionnels de l'(in)sécurité.

Les pratiques contemporaines renvoient donc à présent à des réalités techniques qui méritent d'être réinterrogées en raison non seulement des formes inédites qu'elles sont parfois amenées à revêtir, mais aussi de la particularité des objectifs qui leur sont assignés, ou bien encore de celle des acteurs maintenant impliqués dans leur développement. Et c'est là où l'intensification de certaines pratiques, en faisant système, modifie sans doute en profondeur leur impact en reconfigurant ce que nous appelons société libérale et libertés publiques ¹².

La plupart des contributions ici réunies permettent de souligner justement cet impact en insistant par exemple sur l'essor considérable des entreprises de fichage et de listing qui s'inscrivent actuellement dans un cadre transnational. Elles montrent également que ces initiatives reposent sur une collecte grandissante de données à caractère personnel extrêmement diversifiées, concernant des catégories sans cesse plus vastes d'individus, et sur une exploitation complexe des informations recueillies qu'autorise la mobilisation d'instruments perfectionnés auxquels les pouvoirs publics ne sont plus les seuls à recourir. Elles éclairent de surcroît des *modus operandi* qui semblent non plus unique-

11. Nous pensons notamment au réseau Identinet que coordonnent Jane Caplan et Edward Higgs du Saint Anthony's College (université d'Oxford) : <http://identinet.org.uk/>.

12. Carrera S., Guild E., *Europe's 21st Century Challenge: Delivering Liberty and Security*, Londres, Ashgate, 2010.

ment conditionnés par la seule nécessité de savoir avec certitude qui est qui, mais également par d'autres impératifs érigés en priorités : en particulier le *data mining* et le profilage dans le cadre de la lutte contre le terrorisme. Anthony Amicelle et Gilles Favarel-Garrigues examinent en détail ces enjeux dans le cadre de la lutte contre le financement du terrorisme et du crime organisé, en particulier à travers l'affaire SWIFT. Ils montrent particulièrement bien comment des logiques bureaucratiques contradictoires, des discours politiques généralisateurs, des techniques que l'on tient à appliquer coûte que coûte, des formes de spécialisations professionnelles à l'interface de différents métiers créent un « dispositif » peu effectif dans son objectif de limiter le terrorisme ou le crime organisé, mais très efficace en terme de promotion de logiques professionnelles. Au prix d'ailleurs de la création de situations humaines qui n'ont rien à envier à l'univers kafkaïen. Dans le même registre, mais sur un autre terrain, François Lenfant, Lia van Broekhoven et Frank van Lierde examinent, à travers le cas de l'ONG Cordaid et de son réseau de partenaires dans le monde, ce qu'implique pour les ONG œuvrant dans l'humanitaire et le développement la guerre décrétée contre le terrorisme depuis le 11 septembre 2001 et comment celle-ci entrave leurs actions. Mathijs Le Rutte, quant à lui, insiste sur les difficultés pratiques actuellement rencontrées par les demandeurs d'asile pour pouvoir s'échapper de leur pays et passer les obstacles de la suspicion et de la pré-culpabilité qui les frappe, *via* ces échanges d'informations ciblant des populations entières et n'allant guère dans le sens d'une individualisation effective qui permettrait aussi d'aider ceux qui sont en danger, et qui sont ici confondus avec les individus dangereux.

Les enjeux liés à la présomption d'innocence, à la manière dont il est central de refuser le paradigme de la transparence à l'égard du regard policier afin de préserver une part d'autonomie privée (*privacy*) vont bien au-delà du droit à la rectification de données personnelles erronées ou de droit d'accès aux fichiers. Et c'est ce que montrent très bien les trois articles suivants. Rocco Bellanova et Paul de Hert analysent la jurisprudence récente du cas S. et Marper et comment les cours européennes refusent de se laisser entraîner dans les logiques de la sécurité maximale. Alex Türk, président du groupe de l'article 29 sur la protection des données, et Dick Marty, parlementaire, magistrat et auteur d'un rapport fondamental pour le Conseil de l'Europe, soulignent aussi particulièrement bien, dans leurs entretiens respectifs, qu'il est nécessaire d'aller au-delà de la seule question technique et juridique de la protection des données informatiques et qu'il faut rediscuter les conditions de possibilité discursives qui ont amené certains experts de sécurité à nous présenter le monde comme un monde de danger permanent et global qui justifierait qu'ils puissent agir en tout temps et préventivement. Si tel était le cas, nous sortirions des espaces démocratiques que les luttes pour les droits ont réussi à faire exister, et qui supposent le respect de règles de droit, quand bien même une majorité apeurée peut soutenir le gouvernement du moment. La question posée va donc bien au-delà des tracasseries d'ordre bureaucratique ou des pratiques dis-

criminales subies, ou même des difficultés éprouvées afin de ne plus être répertorié dans certains fichiers à la suite d'inscriptions indues, de situations de privation de droits et de ressources ¹³ ou d'arrestations et de détentions de personnes innocentes ¹⁴, elle touche aux incidences sur le vécu et la trajectoire des individus, à la victimisation de certains, à la réactivation de logiques de bouc émissaire qui viennent elles mêmes de la réapparition de formes de suspicion et de modalités d'action voulant s'exonérer du temps nécessaire à la justice pour rechercher des preuves, au nom de l'urgence et de la prévention.

13. Voir notamment le cas relaté dans l'article « Inscrit sur la liste antiterroriste de l'ONU, un couple belge innocenté, est réduit à une « mort civile » », *Le Monde*, 25 décembre 2008.

14. Dans son avis sur le système d'information Schengen (SIS II), le contrôleur européen de la protection des données évoque par exemple le cas suivant : « En juin 2004, un avocat de Portland (États-Unis) a été emprisonné pendant deux semaines parce que le FBI avait établi que ses empreintes digitales correspondaient à des empreintes trouvées dans le cadre des attentats de Madrid (sur un sac plastique ayant contenu le détonateur). Il a finalement été établi que la technique de comparaison était défectueuse et avait entraîné une erreur d'interprétation », *Journal Officiel de l'Union Européenne*, 19 avril 2006 (C91/44).